

FILED
ASHEVILLE, N.C.**MAR 06 2019****U.S. DISTRICT COURT**
W. DIST. OF N.C.**UNITED STATES DISTRICT COURT**

for the

Western District of North Carolina

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*A Verizon Cell Phone with phone number 919-323-7152
listed in Attachment A currently in the custody of
Jonathan P. SHOEMAKER

Case No. 1:19-mj-37

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Western District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(a)(2)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Klarisa C. Zaffark Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

3/6/2019*Judge's signature*City and state: Asheville, North Carolina

W. Carleton Metcalf, U.S. Magistrate Judge

Printed name and title

MAR 06 2019

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

U.S. DISTRICT COURT
W. DIST. OF N.C.

IN THE MATTER OF THE
SEARCH OF THE FOLLOWING:
A VERIZON CELL PHONE
WITH PHONE NUMBER (919) 323-7152
AND IMEI 3533100833137310
LISTED IN ATTACHMENT A

§
§
§
§
§
§

CASE NO. 1:19mj37

I, Klarisa Zaffark, being duly sworn, depose and state the following:

1. I am a Special Agent (SA) with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed from May 2010, to the present. I am currently assigned to the HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations related to the sexual exploitation of children. I have also received training and instruction in the field of investigating child pornography to include distribution and possession. As part of my duties and responsibilities as an HSI SA, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18 United States Code, Section 2251, et seq.

2. As a result of training and experience, I am familiar with methods employed by individuals engaged in various illegal activities, including interstate transportation of child pornography. I am also aware from my training and experience that persons engaged in interstate transportation of child pornography typically use false identities and other techniques to disguise themselves and their enterprise. I am further aware, as a result of my training and experience that child pornography is not generally available in retail establishments, even from those which offer other explicit sexual material. Persons who wish to obtain child pornography do so by ordering and/or obtaining it by discreet contact with other individuals and underground businesses that have child pornography collections.

3. This investigation involves the distribution and receipt of child pornography across state boundary lines through the use of computers and the Internet. All such transmissions must go through Internet Service Providers servers, where the said Internet Service Provider temporarily stores such transmissions. Additionally, this investigation involves an individual traveling with the intent to engage in illicit sexual conduct with a minor.

4. This affidavit is submitted in support of an application for a search warrant for a Verizon Wireless cell phone (919) 323-7152 / IMEI: 3533100833137310 (the MOBILE DEVICE). The aforementioned device is believed to be in the custody of Johnathan Paul SHOEMAKER.

5. Your Affiant is personally familiar with facts and circumstances surrounding this investigation, both from his own investigative activities, and from information obtained from other law enforcement officers/agencies.

6. As more fully described below, your Affiant has probable cause to believe that presently and/or at the time of this warrant's execution, evidence of child pornography, and evidence linking Johnathan Paul SHOEMAKER to child pornography receipt, distribution, and possession will be found inside the following item: Verizon Wireless cell phone (919) 323-7152 / IMEI: 3533100833137310. I have reason to believe these items will be found inside the MOBILE DEVICE and constitute evidence of the commission of the crime of certain activities relating to production of child pornography in violation of Title 18, United States Code, § 2252A(a)(5)(B) - possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography; and Title 18, United States Code, § 2252A(a)(2)(A) – knowingly distributed and received child pornography. Such items are evidence, contraband, the fruits of crime and things otherwise criminally possessed, property designated or intended for use or which is or has been used as the means of committing a criminal offense.

7. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 2252A(a)(2), (a)(5)(B), which relate to the knowing distribution and possession of child pornography is presently located in the above listed items.

RELEVANT STATUTES

8. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252A(a)(2) and (a)(5)(B), relating to material involving the sexual exploitation of minors.

9. Title 18 U.S.C. § 2252A(a)(2) makes it a federal offense for any person to knowingly distribute or receive in interstate or foreign commerce by any means, including by computer, any visual depiction if such visual depiction involves the use of a minor engaging in sexually explicit conduct. Section 2252A(a)(2) makes it a federal crime for any person to knowingly receive or distribute child pornography that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means, including computer, or knowingly reproduce any visual depiction for distribution in interstate or foreign commerce by any means, including by computer, or through the mail. Section 2252A(a)(5)(B) makes it a federal crime for any person to knowingly possess, or access with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer.

DEFINITIONS

10. The following definitions apply to this Affidavit:

11. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

12. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

13. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

14. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

15. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user

name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

16. An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

17. “Log Files” are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

18. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

19. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport

Protocol (HTTP).

20. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

21. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

22. "Smart Phone", a Smart Phone is a mobile phone that utilizes a mobile operating system similar to the way a traditional computer uses an operating system to function. Smart Phones are typically capable of storing various types of media files, including image, video and audio files; of accessing the Internet through wireless or cellular data connections and Internet

browsing software; of capturing still images and video through integrated cameras built into the device; of accessing electronic mail accounts; and providing services utilizing the Global Positioning System.

23. "Memory Card", a memory card or flash card is an electronic flash memory data storage device used for storing digital information. They are commonly used in many electronic devices, including digital cameras, mobile phones, laptop computers, MP3 players and video game consoles. They are small, re-recordable, and able to retain data without power.

BACKGROUND REGARDING SEIZURE OF COMPUTERS

24. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

25. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

26. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and

its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

27. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

28. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and

other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

BACKGROUND REGARDING THE INTERNET

29. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately September 1998. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

30. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The

ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

31. Photographs and other images can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner", which is an optical device that can recognize characters on paper and, by using specialized software, convert them to digital form. Storage can also be captured from single frames of video and converted to an image file. After the photograph or other image has been scanned into the computer, the computer can store the data from the image as an individual "file". Such a file is known as an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

32. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte (1,000 gigabytes) are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

33. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer.

The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and or print out a hard copy of the image by using a printer device (such as a laserjet or inkjet).

34. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION

35. On or about January 9, 2019, HSI Hendersonville, North Carolina Special Agents (SAs) were contacted by the Henderson County Sheriff's Office (HCSO) for assistance after received an investigative lead from the Alachua County Sheriff's Office (ACSO) located in Florida.

I received the following information provided by HCSO concerning the facts of the investigation:

36. An investigation by the ACSO revealed an eleven (11) year-old victim residing in Gainesville, Florida was sexually exploited via the Internet by a suspect believed to be residing in Western North Carolina. The investigation revealed that the victim, herein referred to as victim one "VM1", communicated with a suspect via a messaging application named KIK while utilizing her Samsung Optimus Zone 3 cellular phone. According to the website <http://KIK.com/about>, KIK advertises itself as "the first smartphone messenger with a built-in browser." KIK Messenger allows its users to "talk to your friends and browse and share any web site with your friends on KIK." KIK believes it is at the forefront of the "new era of the mobile web." KIK was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." KIK Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, KIK usernames - not phone numbers - are the basis for KIK user accounts, so KIK users are in complete control with whom they communicate. In addition, KIK features include more than instant messaging. KIK users can exchange images, videos, sketches, stickers and even more with mobile web pages. Kik can also be installed on a

computer, laptop, or tablet.

37. On June 20, 2018, ACSO investigators traveled to VM1's residence after receiving information that lewd and lascivious digital images were being sent by VM1 to unidentified individuals while utilizing the KIK application. The investigation revealed VM1 communicated with a suspect on KIK associated with the KIK username "Froggydogg88." VM1 informed ACSO investigators that she had been communicating with "Froggydogg88" and an additional KIK user for approximately one (1) week. VM1 informed investigators that "Froggydogg88" stated he was eighteen (18) years-old.

38. On this same date, VM1's mother provided investigators with verbal and written consent to search VM1's cellular device. As a result of the search, it was observed that the first conversation between the victim and the suspect appears on the victim's device as June 16, 2018. During this conversation, it appears as though VM1 sent multiple digital attachments to "Froggydogg88" but these attachments were not recovered during the data extraction of the cellular device. A review of the extraction report revealed the digital attachments sent by VM1 were either labeled as "Empty File" or displayed as blank on the extraction report. Communication between VM1 and "Froggydogg88" prior to and after the digital attachments were sexually explicit in nature. The excerpts in the following paragraphs were indicative of the conversations.

39. The following is an excerpt of messages exchanged between VM1 and "Froggydogg88" via the KIK application on June 16, 2018.

VM1 to "Froggydogg88": "Hru"

"Froggydogg88" to VM1: "Ready to be out of this car already"

VM1 to "Froggydogg88": "Ha I bet"

"Froggydogg88" to VM1: "Wyd"

VM1 to "Froggydogg88": "Laying"

"Froggydogg88" to VM1: "Wearing"

VM1 to "Froggydogg88": *Blank Message believed to previously contain digital attachment*

"Froggydogg88" to VM1: "U sent that last night. Lol"

VM1 to "Froggydogg88": "Ya I never changed"

"Froggydogg88" to VM1: "Gotcha"

VM1 to "Froggydogg88": "What r u wearing love"

"Froggydogg88" to VM1: "Shirt and shorts"

VM1 to "Froggydogg88": "Ha"

"Froggydogg88" to VM1: "Boring"

"Froggydogg88" to VM1: "I'll be able to be naughty late tonight though"

VM1 to "Froggydogg88": "Mmmm"

"Froggydogg88" to VM1: "I love your tits btw"

"Froggydogg88" to VM1: "And I want you to surprise me. Be creative :)"

40. On this same date, several hours later, the victim and suspect continued to communicate. The following is an excerpt of messages exchanged between VM1 and "Froggydogg88" via the KIK application on June 16, 2018.

VM1 to "Froggydogg88": "Empty File" *Contains digital attachment*

VM1 to "Froggydogg88": *Blank Message believed to previously contain digital attachment*

VM1 to "Froggydogg88": "Empty File" *Contains digital attachment*

"Froggydogg88" to VM1: "Yes"

"Froggydogg88" to VM1: "The those shorts off"

VM1 to "Froggydogg88": *Blank Message believed to previously contain digital attachment*

"Froggydogg88" to VM1: "Yessss"

"Froggydogg88" to VM1: "Put on leg on the counter and spread"

"Froggydogg88" to VM1: "Make it a video of leg on counter rubbing your pussy"

VM1 to "Froggydogg88": *Blank Message believed to previously contain digital attachment*

VM1 to "Froggydogg88": *Blank Message believed to previously contain digital attachment*

"Froggydogg88" to VM1: "That's perfect"

42. A review of the extraction report provided by ACSO investigators of VM1's cellular device revealed a video file discovered in the Media/Internal/storage/DCIM/Camera section of the device. The video appears to have been created on June 19, 2018 at approximately 07:40:13 PM (UTC-4). The video depicts VM1 utilizing a cellular device to record herself while fully nude with one leg on what appears to be a bathroom countertop. VM1 is observed holding the cellular device with one hand and rubbing her vaginal area with the other hand.

43. As the above-mentioned June 19, 2018 conversation continued, 'Froggydogg88' asks VM1 "Can you delete this while conversation and show me please". VM1 responds to "Froggydogg88" with a screenshot containing a blank screen while in the KIK application.

44. The victim and suspect continue to communicate on June 19, 2018. The following is a continued excerpt of messages exchanged between VM1 and "Froggydogg88" via the KIK application on June 19, 2018.

VM1 to "Froggydogg88": "Ya can u video chat"

"Froggydogg88" to VM1: "No. All my lights are off"

VM1 to "Froggydogg88": "So all u need to see is me and to just talk to me"

"Froggydogg88" to VM1: "But you wont see me"

VM1 to "Froggydogg88": "Go to the bathroom then I can see u"

"Froggydogg88" to VM1: "Lol I just need your voice for now baby"

VM1 to "Froggydogg88": "K I just need your voice for now baby"

"Froggydogg88" to VM1: "What if your mom walks in"

VM1 to "Froggydogg88": "Turn you phone of"

VM1 to "Froggydogg88": "Off"

"Froggydogg88" to VM1: "But you will be doing naughty stuff and she will see"

45. On June 20, 2018, at approximately 12:46:52 AM (UTC-4), VM1 sent "Froggydogg88" a digital image depicting a close-up of her hands spreading open her vaginal area. VM1 followed the above message and sent "Froggydogg88" two additional sexually explicit digital images.

46. On July 9, 2018, ACSO Detective Robert Campbell, submitted a subpoena to Kik Interactive, Inc. requesting all subscriber information pertaining to the Kik user account of "Froggydogg88".

47. On or about July 10, 2018, ACSO Detective Campbell received a response from Kik Interactive, Inc. in reference to the Customs summons submission for Kik account:

“Froggydogg88”. KIK Interactive, Inc. provided the following information:

First Name: Froggy

Last Name: D

Email: jshoemaker88@gmail.com (confirmed)

Username: Froggydogg88

48. Results revealed that user “Froggydogg88” registered with Kik as a user on August 14, 2014 and while utilizing a Motorola Moto Z Android cellular phone.

49. KIK provided IP logs for the user “Froggydogg88” from 06/10/2018 through 07/10/2019. During the given timeframe investigators identified one (1) IP address logged on numerous occasions and listed as 68.115.217.106.

50. On July 11, 2018, ACSO Detective Campbell submitted a subpoena to Google LLC., requesting all subscriber information pertaining to the email account of “jshoemaker88@gmail.com”.

51. On August 17, 2018, ACSO Detective Campbell received a response from Google LLC., in reference to the subpoena submission for Google email account:

“jshoemaker88@gmail.com”. Google LLC. provided the following information:

Name: Jon Shoemaker

E-mail: Jshoemaker88@gmail.com

Recovery E-mail: Jonathan.shoemaker@duke.edu

Created On: 2007/08/17-15:47:21-UTC

SMS: 919-323-7152

52. On August 17, 2018, ACSO Detective Campbell submitted a subpoena to Duke University requesting all subscriber information pertaining to the email account of "Jonathan.shoemaker@duke.edu".

53. On August 20, 2018, received a response from Duke University in reference to the subpoena submission to Duke University for subscriber information on "Jonathan.shoemaker@duke.edu". Results revealed the following information:

Duke Unique ID: 0450419

Social SN: XXX-XX-6387

Date of Birth: 03/20/1984

Continuous Service Date: 7/23/2007

Termination Date: 10/6/2014 (Voluntary resignation)

54. Utilizing a law enforcement investigative tool, SA Zaffark queried telephone number "919-323-7152" previously identified as associated with the suspects email account. The query resulted in the above-mentioned phone number associated to a Jonathan Paul Shoemaker (SHOEMAKER) with a date of birth of March 20, 1984, with associated utilities at 93 Farm Lane, Asheville, NC 28759.

55. On January 8, 2019, after determining the IP address 68.115.217.106 was owned by Charter Communications, Inc., a Customs summons was sent for subscriber information related to the account. Charter Communications, Inc., responded to the summons with legal compliance and identified the above-mentioned IP address as subscribed to Mission Hospital located at 980 Hendersonville Road, Asheville, North Carolina 28803.

56. Utilizing a law enforcement investigative tool, it was discovered SHOEMAKER is an employee at Memorial Mission Hospital Inc. located in Asheville, NC.

57. On January 8, 2019, HSI Intelligence Research Specialist (IRS) Amy Storer, on behalf of SA Zaffark, submitted a Customs summons to Kik Interactive, Inc. requesting updated subscriber information pertaining to the Kik user account of "Froggydogg88."

58. On January 9, 2019, SA Zaffark received a response from Kik Interactive, Inc. in reference to the Customs summons submission for Kik account: "Froggydogg88". KIK Interactive, Inc. provided the following information:

First Name: Froggy

Last Name: D

Email: jshoemaker88@gmail.com (confirmed)

Username: Froggydogg88

59. Results from Kik included IP logs for the user "Froggydogg88" from 12/10/2018 through 01/09/2019. Results revealed that identical information previously identified by ACSO Detectives original subpoena results listed above. Additionally, results revealed "Froggydogg88" was most recently captured by Kik utilizing the application as of January 9, 2019.

60. On January 14, 2019, HSI Intelligence Research Specialist (IRS) Amy Storer, on behalf of SA Zaffark, submitted a Customs summons to Morris Broadband requesting all subscriber and customer information associated to the address 93 Farm Lane Mills, River, North Carolina, 28759.

61. On January 21, 2019, Morris Broadband responded to the order with legal compliance. Results revealed the following information:

Billing Account: 085396

First Name: JONATHON

Last Name: SHOEMAKER

Physical Address: 93 FARM LN MILLS RIVER NC 28759-4642

Billing Address: Same as Physical Address

Telephone Number: (919) 323-7152

E-Mail Address: jshoemaker88@gmail.com

Customer Since: 08/04/2015

Modem MAC: 18:9C:27:CB:FD:5D

CPE MAC: 24:f5:a2:44:89:ec

IP Address: Current IP is being assigned by dynamic CG-NAT (Carrier Grade Network Address Translation) and can change at any given time.

62. In February 2019, SA Zaffark conducted open source checks and linked SHOEMAKER to a Facebook account under the name "Jon Frogg Shoemaker". The following information was observed in the "Intro" section of the webpage:

Facebook Identifier: www.facebook.com/jon.f.shoemaker

Facebook Header: Jon Frogg Shoemaker

Educator at: Mission Health

Pediatrics at: Duke Hospital

Studied Psychology at: UNC Asheville

Lives in: Asheville, North Carolina

From: Palm Beach Gardens, Florida

63. On February 21, 2019, HSI Intelligence Research Specialist (IRS) Amy Storer, on behalf of SA Zaffark, submitted a Customs summons to Verizon Wireless requesting all subscriber and call information associated to the telephone number (919) 323-7152.

64. On February 26, 2019, SA Zaffark received a response from Verizon Wireless in

response to the Customs Summons. Verizon Wireless provided the following subscriber information assigned to telephone number (919) 323-7152:

Account Number: 921027794-1

Last Name: Shoemaker

First Name: Jonathan

Middle: P

Address: 93 Farm Ln., Mills River, NC 28759

Phone No. 1: (919) 323-7152

Phone No. 2: (919) 416 2445

MTN Effective Date: 9/12/2007

CONCLUSION

65. Based on the foregoing facts, I respectfully submit that there is probable cause to believe child pornography, as set forth in the search warrant, will be found on the MOBILE DEVICE. Furthermore, there is probable cause to believe that evidence linking Jonathan Paul SHOEMAKER to the following will be found on this device:

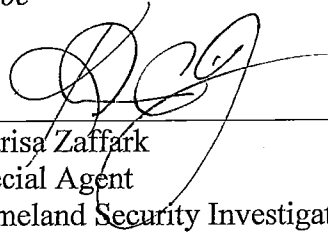
- a. the pseudonym: "Froggydog88";
- b. the particular messaging application and other applications;
- c. the IP addresses mentioned in the affidavit linking to SHOEMAKER's place of employment;
- d. the Facebook.com pseudonym "Frogg" as identified in SHOEMAKER's Facebook Header

66. Your Affiant respectfully requests that a warrant be issued authorizing HSI Special

Agents, with appropriate assistance from other law enforcement personnel and/or agencies to seize the MOBILE DEVICE and search the above referenced items as more specifically described in ATTACHMENT B.


67. Since the IMEI and the phone number are not apparent from examining the exterior of a cellular phone, I further request to be authorized to make an initial inspection of any cellular phone located in the custody of Jonathan Shoemaker for the purpose of determining its IMEI and phone number prior to conducting an in depth search for the items described in ATTACHMENT B.

Reviewed by Assistant United States Attorney David A. Thorne



Klarisa Zaffark
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 6 day of March 2019.



W. CARLETON METCALF
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF NORTH CAROLINA

ATTACHMENT A

SUBJECT PROPERTY TO BE SEARCHED

One (1) Verizon Wireless cell phone (919) 323-7152 / IMEI: 3533100833137310
MOBILE DEVICE, believed to be in the custody of Johnathan Paul SHOEMAKER.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All electronic files containing child pornography and images of child pornography in any form, information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256 and records or other items which evidence ownership or use of computer that is currently saved on the MOBILE DEVICE.
2. Records, documents, writings, and correspondences with others pertaining to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
3. Any and all, photographs, letters, written narratives and computer text files or electronic matter to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.
4. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the item described in Attachment A.
5. Electronic mail, chat logs, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.
6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage,

including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Storage combinations, and passwords, which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of child pornography.
8. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
9. Visual depictions, in whatever form, including digital, of minors engaged in sexually explicit conduct.
10. Records or data in any form relating to the following:
 - a. the pseudonym: "Froggydogg88";
 - b. the particular messaging application and other applications;
 - c. the IP addresses mentioned in the affidavit linking to SHOEMAKER's place of employment;
 - d. the Facebook.com pseudonym "Frogg" as identified in SHOEMAKER's Facebook Header